CLAIMS

1. A method for a gaming terminal to authorize execution of downloaded software, comprising the steps of:

running in the gaming machine a version of Microsoft Windows operating system having Software Restriction Policy capability, and

setting the Software Restriction Policy to authorize execution of software code-signed with a certificate from a designated trusted party.

2. The method of claim 1, wherein the running step runs a version of Microsoft Windows operating system having System File Protection capability.

3. The method of claim 1, wherein the running step runs a version of Microsoft Windows operating system having Driver Signing capability.

4. The method of claim 3, further comprising the step of:

setting the Microsoft Driver Signing policy to only authorize execution of drivers code-signed with a certificate from Microsoft.

5. The method of claim 3, further comprising the step of:

setting the Microsoft Driver Signing policy to only authorize execution of drivers that are code-signed with a certificate from at least one of Microsoft and a designated trusted party.

6. The method of claim 1, wherein the running step runs a version of Microsoft Windows operating system having System File Protection and Driver Signing capabilities.

7. The method of claim 1, wherein the gaming machine includes a processing hardware and wherein the processing hardware and the operating system in the running step collectively implement Microsoft's Palladium capability.

8. The method of claim 1, wherein the gaming machine includes a

processing hardware and wherein the operating system in the running step is a Microsoft Windows operating system that, together with the processing hardware, implements Microsoft's Palladium, Windows File Protection and Driver Signing capabilities.

9. The method of claim 1, wherein the gaming machine includes a processing hardware and wherein the operating system in the running step is a version of Microsoft Windows operating system that, together with the processing hardware, implements capabilities specified by the Trusted Computing Platform Alliance (TCPA).

10. The method of claim 1, wherein the gaming machine includes a processing hardware and wherein the operating system in the running step is a version of Microsoft Windows operating system that, together with the processing hardware, implements TCPA, System File Protection or Windows File Protection and Driver Signing.

11. A method for a gaming terminal to authorize execution of downloaded software, comprising the steps of:

running an operating system that includes a configurable policy functionality for restricting code execution to code that has been signed by a designated trusted party;

configuring the restricting policy functionality to only authorize execution of software that is code-signed with a certificate from the designated trusted party.

12. The method of claim 11, wherein the restricting policy functionality conforms to the Microsoft Software Restriction Policy.

13. The method of claim 11, wherein the operating system in the running step is configured to prevent a replacement of selected monitored or protected system files with files that do not originate from a trusted source.

14. The method of claim 13, wherein the trusted source is the designated trusted party.

15. The method of claim 13, wherein the operating system includes one of

Microsoft's System File Protection (SFP) and Microsoft's Windows File Protection (WFP).

16. The method of claim 1, wherein the operating system in the running step is configured to only allow execution of drivers that have been code-signed with a certificate from a trusted source.

17. The method of claim 16, wherein the operating system includes Microsoft's Driver Signing and wherein the trusted source is Microsoft.

18. The method of claim 11, wherein the operating system in the running step is configured to:

prevent a replacement of selected monitored or protected system files with files that do not originate from a trusted source, and

only allow execution of drivers that have been code-signed with a certificate from the trusted source.

19. The method of claim 18, wherein the trusted source is Microsoft.

20. The method of claim 18, wherein the operating system in the running step incorporates Microsoft's Driver Signing and one of Microsoft's System File Protection (SFP) and Microsoft's Windows File Protection (WFP).

21. The method of claim 11, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implement a Palladium-like capability.

22. The method of claim 11, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements a Palladium-like, System File Protection and Driver Signing capabilities.

23. The method of claim 11, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step,

implements capabilities specified by the Trusted Computing Platform Alliance (TCPA).

24. The method of claim 1, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements TCPA, and Microsoft's Windows File Protection and Driver Signing.

25. A method for operating a gaming machine comprising the steps of:

running an operating system loaded in the gaming machine;

downloading at least one software module into the gaming machine;

checking a code signature of at least one downloaded software module using a trusted verification driver, and

authorizing execution of the downloaded software module in the gaming machine only if the downloaded software module is successfully verified by the trusted verification driver.

26. The method of claim 25, wherein the running step runs an operating system that is configured to prevent a replacement of selected monitored or protected system files within the gaming machine with files that do not originate from a trusted source.

27. The method of claim 25, wherein the running step runs an operating system that is configured to prevent the execution of selected monitored or protected system files within the gaming machine for files that do not originate from a trusted source.

28. The method of claim 25, wherein the running step runs an operating system whose capability includes one of Microsoft's System File Protection (SFP) and Microsoft's Windows File Protection (WFP).

29. The method of claim 25, wherein the operating system in the running step causes the authorizing step to authorize execution of the downloaded software module only if the downloaded software module has been code-signed with a certificate from a trusted source.

30. The method of claim 29, wherein the running step runs an operating system that includes Microsoft's Driver Signing and wherein the trusted source is Microsoft.

31. The method of claim 29, wherein the running step runs an operating system that includes Microsoft's Driver Signing.

32. The method of claim 30, wherein the downloaded software module includes a driver and wherein the method further comprises the step of:

setting a Microsoft Driver Signing policy to cause the authorizing step to only authorize execution of drivers that are code-signed with a certificate from one of Microsoft and a trusted source.

33. The method of claim 25, further comprising the step of:

setting a Microsoft Driver Signing policy,

and authorizing the installation and execution of the trusted verification driver subsequent to verifying that it is code-signed with a certificate from a trusted source.

34. The method of claim 32a, wherein the trusted source is Microsoft.

35. The method of claim 30a, further comprising the step of:

setting a Microsoft Driver Signing policy to cause the authorizing step to only authorize execution of drivers that are code-signed with a certificate from at least one of Microsoft and a designated trusted source.

36. The method of claim 25, wherein the operating system in the running step is a Microsoft Windows operating system configured with Software Restriction Policy, Windows File Protection and Driver Signing

37. The method of claim 25, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements Microsoft's Palladium capability.

38. The method of claim 25, wherein the operating system in the running step is a Microsoft Windows operating system configured with Software Restriction Policy, Windows File Protection and Driver Signing and wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements Microsoft's Palladium capability.

39. The method of claim 25 wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements Microsoft's Palladium, Software Restriction Policy, Windows File Protection and Driver Signing capabilities.

40. The method of claim 25, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements capabilities specified by the Trusted Computing Platform Alliance (TCPA).

41. The method of claim 40, wherein the operating system in the running step is a Microsoft operating system.

42. The method of claim 25, wherein the operating system in the running step is a Microsoft operating system implementing TCPA, Software Restriction Policy, Windows File Protection and Driver Signing.

43. The method of claim 25, wherein the operating system in the running step is a Microsoft Windows operating system configured with Software Restriction Policy, Windows File Protection and Driver Signing and wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements the Trusted Computing Platform Alliance (TCPA) specification.

44. The method of claim 25, wherein the operating system in the running step is a an operating system configured with Software Restriction Policy, System File Protection and Driver Signing and wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements Palladium-like capability.

45. The method of claim 25, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements Palladium-like capability.

46. The method of claim 25, wherein the operating system in the running step is a Microsoft Windows operating system configured with Software Restriction Policy, Windows File Protection and Driver Signing and wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements Palladium-like capability.

47. A method for verifying gaming terminal software, comprising the steps of:

installing at least one driver into the gaming machine;

taking complete control of the gaming machine with the at least one driver;

verifying a legitimacy of all software and memory content in the gaming machine;

relinquishing control of the gaming machine, and

authorizing the gaming machine to execute only of the software that is successfully verified.

48. The method of claim 47, whereby the at least one driver is configured to execute at a highest machine permission level.

49. The method of claim 47, wherein the taking step includes a step of freezing an operation of the operating system.

50. The method of claim 47, wherein the taking step includes a step of blocking the execution of the operating system.

51. The method of claim 47, wherein the taking step includes a step of disabling interrupts on the gaming machine.

52. The method of claim 47, wherein the verifying step includes verifying a BIOS of a motherboard of the gaming machine.

53. The method of claim 47, wherein the verifying step includes verifying a BIOS of any add-on board within the gaming machine.

54. The method of claim 47, wherein the verifying step includes verifying ROM shadowing within the gaming machine.

55. The method of claim 47, wherein the verifying step includes verifying hardware registers.

56. The method of claim 47, wherein the verifying step includes verifying a signature in memory of the at least one driver.

57. The method of claim 47, wherein the verifying step includes verifying a content of files on disk within the gaming machine.

58. The method of claim 47, wherein the verifying step includes verifying a downloadable micro-code of smart hardware within the gaming machine.

59. The method of claim 47, wherein the verifying step includes verifying a downloadable firmware of a smart hardware within the gaming machine.

60. The method of claim 47, further comprising the step of auditing a source code of the at least one driver by a third party.

61. The method of claim 47, further comprising the step of auditing a source code of the at least one driver by a game certification lab.

62. The method of claim 47, further comprising the step of certifying the at least one driver by a game certification lab.

63. The method of claim 47, further comprising the step of code-signing with a certificate the at least one driver by a game certification lab.

64. The method of claim 47, further comprising the step of certifying the at least one driver by a third party.

65. The method of claim 47, further comprising the step of code-signing with a certificate the at least one driver by a third party.

66. The method of claim 47, wherein the gaming machine is controlled by a PC, wherein the at least one driver is code signed and wherein the installing step installs the code-signed driver, the installing step being triggered by at least one plug-and-play dongle inserted in at least one port of the PC.

67. The method of claim 47, wherein the at least one driver installed in the installing step is code-signed by Microsoft's WHQL.

68. The method of claim 47, wherein the verifying step verifies the legitimacy of the software and memory contents without modifying a content thereof and wherein the method further includes a step of reporting an outcome of the verifying step.

69. The method of claim 47, wherein the verification step includes a challenge-response step to ensure that the trusted verifier driver has not been spoofed.

70. The method of claim 47, wherein the verification step includes a challenge-response step to ensure that the trusted verifier driver is executing.

71. The method of claim 47, wherein the gaming machine further includes a third party dongle installed therein and wherein the at least one driver is linked to the third party dongle to enable the third party to audit the at least one driver.

72. The method of claim 47, wherein the gaming machine further includes an interface for a dongle compliant with the Microsoft plug and play specification and

wherein the at least one driver is installed or activated when the dongle is plugged-in.

73. The method of claim 47, wherein the gaming machine further includes a hard disk drive that includes at least one partition formatted for simple file access and wherein the method further includes a step of accessing code-signed downloaded software from the at least one simple file access partitioned hard disk drive.

74. The method of claim 73, wherein the hard disk drive partition is formatted according to FAT32 protocol.

75. The method of claim 73, wherein the hard disk drive partition is formatted according to a predetermined file format protocol.

76. The method of claim 47, wherein the gaming machine further includes a plurality of hard disk drives wherein at least one hard disk drive contains at least one partition formatted for simple file access and wherein the method further includes a step of accessing code-signed downloaded software from the at least one partition formatted for simple file access.

77. The method of claim 73, wherein the at least one partition is formatted according to FAT32 protocol.

78. The method of claim 73, wherein the at least one partition is formatted according to a predetermined file format protocol.

79. The method of claim 47, wherein the verifying step verifies the memory content or a trusted signature of the memory content stored on at least one of:

a hard disk drive of the gaming machine,
an optical memory of the gaming machine,
flash memory of the gaming machine,
non-volatile RAM memory of the gaming machine,
registers of integrated circuits of the gaming machine,
ferromagnetic memory of the gaming machine,

magnetic memory of the gaming machine,
ROM memory of the gaming machine,
OTP memory of the gaming machine,
holographic memory of the gaming machine, and
firmware of a smart peripheral.

80. A gaming machine, comprising:
at least one processor;
at least one data storage device;
a plurality of processes spawned by the at least one processor, the processes including processing logic for carrying out steps of:
running an operating system loaded in the gaming machine;
downloading at least one software module into the gaming machine;
checking a code signature of at least one downloaded software module using a trusted verification driver, and
authorizing execution of the downloaded software module in the gaming machine only if the downloaded software module is successfully verified by the trusted verification driver.

81. The gaming machine of claim 80, wherein the running step runs an operating system that is configured to prevent a replacement of selected monitored or protected system files within the gaming machine with files that do not originate from a trusted source or that are not consistent with the authorized version of the operating system.

82. The gaming machine of claim 80, wherein the running step runs a Microsoft operating system configured with Windows File Protection (WFP).

83. The gaming machine of claim 80, wherein the operating system in the running step causes the authorizing step to authorize execution of the downloaded software module only if the downloaded software module has been code-signed with a certificate from a trusted source.

84. The gaming machine of claim 83, wherein the running step runs a Microsoft operating system configured with Driver Signing and wherein the trusted source is Microsoft.

85. The gaming machine of claim 83, wherein the running step runs a Microsoft operating system configured with Driver Signing.

86. The gaming machine of claim 80, wherein the downloaded software module includes a driver and wherein the method further comprises the step of:

setting a Microsoft Driver Signing policy to cause the authorizing step to only authorize execution of drivers that are code-signed with a certificate from Microsoft.

87. The method of claim 84, further comprising the step of:

setting a Microsoft Driver Signing policy to cause the authorizing step to only authorize execution of drivers that are code-signed with a certificate from at least one of Microsoft and a designated trusted source.

88. The gaming machine of claim 80, wherein the operating system in the running step is a Microsoft Windows operating system configured with Windows File Protection and Driver Signing.

89. The gaming machine of claim 80, wherein the operating system in the running step is a Microsoft Windows operating system configured with Software Restriction Policy, Windows File Protection and Driver Signing.

90. The gaming machine of claim 80, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements Microsoft's Palladium capability.

91. The gaming machine of claim 80, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements Palladium-like capability.

92. The gaming machine of claim 80, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements Microsoft's Palladium, Software Restriction Policy, Windows File Protection and Driver Signing capabilities.

93. The gaming machine of claim 80, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements Microsoft's Palladium, Windows File Protection and Driver Signing capabilities.

94. The gaming machine of claim 80, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements capabilities specified by the Trusted Computing Platform Alliance (TCPA).

95. The gaming machine of claim 80, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements capabilities specified by the Trusted Computing Platform Alliance (TCPA), Software Restriction Policy, System File Protection and Driver Signing.

96. The gaming machine of claim 80, wherein the gaming machine includes a processing hardware that, together with a Microsoft operating system in the running step, implements capabilities specified by the Trusted Computing Platform Alliance (TCPA), Software Restriction Policy, Windows File Protection and Driver Signing.

97. The gaming machine of claim 94, wherein the operating system in the running step is a Microsoft operating system.

98. The gaming machine of claim 80, wherein the operating system in the running step is a Microsoft operating system implementing TCPA, Software Restriction Policies, Windows File Protection and Driver Signing.

99. The gaming machine of claim 80, wherein the operating system in the running step is a Microsoft operating system implementing TCPA, Windows File

Protection and Driver Signing.

100. The gaming machine of claim 80, wherein the operating system in the running step includes the Software Restriction Policy capability.

101. A gaming machine, comprising:

at least one processor;

at least one data storage device;

a plurality of processes spawned by the at least one processor, the processes including processing logic for carrying out steps of:

installing at least one driver into the gaming machine;

taking complete control of the gaming machine with the at least one driver;

verifying a legitimacy of all software and memory content in the gaming machine;

relinquishing control of the gaming machine, and

authorizing the gaming machine to execute only of the software that is successfully verified.

102. The gaming machine of claim 101, whereby the at least one driver is configured to execute at a highest machine permission level.

103. The gaming machine of claim 101, wherein the taking step includes a step of freezing an operation of the operating system.

104. The gaming machine of claim 101, wherein the taking step includes a step of blocking the operation of the operating system.

105. The gaming machine of claim 101, wherein the taking step includes a step of disabling interrupts on the gaming machine.

106. The gaming machine of claim 101, wherein the verifying step includes verifying a BIOS of a motherboard of the gaming machine.

107. The gaming machine of claim 101, wherein the verifying step includes verifying a BIOS of any add-on board within the gaming machine.

108. The gaming machine of claim 101, wherein the verifying step includes verifying ROM shadowing within the gaming machine.

109. The gaming machine of claim 101, wherein the verifying step includes verifying hardware registers.

110. The gaming machine of claim 101, wherein the verifying step includes verifying a signature in memory of the at least one driver.

111. The gaming machine of claim 101, wherein the verifying step includes verifying a content of files on disk within the gaming machine.

112. The gaming machine of claim 101, wherein the verifying step includes verifying a downloadable micro-code of smart hardware within the gaming machine.

113. The gaming machine of claim 101, wherein the verifying step includes verifying a downloadable firmware of a smart hardware within the gaming machine.

114. The gaming machine of claim 101, further comprising the step of auditing a source code of the at least one driver by a third party.

115. The gaming machine of claim 101, further comprising the step of auditing a source code of the at least one driver by a game certification lab.

116. The gaming machine of claim 101, further comprising the step of certifying the at least one driver by a game certification lab.

117. The gaming machine of claim 101, further comprising the step of code-signing with a certificate the at least one driver by a game certification lab.

118. The gaming machine of claim 101, further comprising the step of certifying the at least one driver by a third party.

119. The gaming machine of claim 101, further comprising the step of code-signing with a certificate the at least one driver by a third party.

120. The gaming machine of claim 101, wherein the processing hardware forms part of a PC that is configured to control the gaming machine and wherein the gaming machine further includes a plug and play dongle inserted in at least one port of the PC, and wherein the at least one driver is code signed and wherein the installing step installs the code-signed driver, the installing step being triggered by the at least one plug-and-play dongle.

121. The gaming machine of claim 101, wherein the at least one driver installed in the installing step is code-signed by Microsoft's WHQL.

122. The gaming machine of claim 101, wherein the verifying step verifies the legitimacy of the software and memory contents without modifying a content thereof and wherein the plurality of processes include a process to report an outcome of the verifying step.

123. The method of claim 101, wherein the verification step includes a challenge-response step to ensure that the trusted verifier driver has not been spoofed.

124. The method of claim 101, wherein the verification step includes a challenge-response step to ensure that the trusted verifier driver is executing.

125. The gaming machine of claim 101, wherein the gaming machine further includes a third party dongle installed therein and wherein the at least one driver is linked to the third party dongle to enable the third party to audit the at least one driver.

126. The gaming machine of claim 101, wherein the gaming machine further includes an interface for a dongle compliant with the Microsoft plug and play

specification and wherein the at least one driver is installed or activated when the dongle is plugged-in.

127. The gaming machine of claim 101, wherein the gaming machine further includes a hard disk drive that includes at least one a partition formatted for simple file access and wherein the plurality of processes include a process to access code-signed downloaded software from the at least one simple file access partitioned hard disk drive.

128. The gaming machine of claim 127, wherein the hard disk drive partition is formatted according to FAT32 protocol.

129. The gaming machine of claim 127, wherein the hard disk drive partition is formatted according to a predetermined file format protocol.

130. The gaming machine of claim 101, wherein the gaming machine further includes a plurality of hard disk drives wherein at least one hard disk drive contains at least one partition formatted for simple file access and wherein the method further includes a step of accessing code-signed downloaded software from the at least one partition formatted for simple file access.

131. The gaming machine of claim 128b, wherein the at least one partition is formatted according to FAT32 protocol.

132. The gaming machine of claim 128b, wherein the at least one partition is formatted according to a predetermined file format protocol.

133. The gaming machine of claim 101, wherein the verifying step verifies the memory content or a trusted signature of the memory content stored on at least one of:

a hard disk drive of the gaming machine,
an optical memory of the gaming machine,
flash memory of the gaming machine,
non-volatile RAM memory of the gaming machine,
registers of integrated circuits of the gaming machine,

ferromagnetic memory of the gaming machine,
magnetic memory of the gaming machine,
ROM memory of the gaming machine,
OTP memory of the gaming machine,
holographic memory of the gaming machine, and
firmware of a smart peripheral.

134. A method for a gaming terminal to authorize execution of downloaded software, comprising the steps of:

running in the gaming machine a version of an operating system having Software Restriction Policy capability, and

setting the Software Restriction Policy to authorize execution of software code-signed with a certificate from a designated trusted party.

135. The method of claim 134, wherein the running step runs a version of the operating system having System File Protection capability.

136. The method of claim 134, wherein the running step runs a version of the operating system having Driver Signing capability.

137. The method of claim 135, further comprising the step of:

setting the Driver Signing policy to only authorize execution of drivers that are code-signed with a certificate from a designated trusted party.

138. The method of claim 134, wherein the running step runs a version of the operating system having System File Protection and Driver Signing capabilities.

139. The method of claim 134, wherein the gaming machine includes a processing hardware and wherein the processing hardware and the operating system in the running step collectively implement Palladium-like capability.

140. The method of claim 134, wherein the gaming machine includes a processing hardware and wherein the operating system in the running step is an operating

system that, together with the processing hardware, implements Palladium-like, System File Protection and Driver Signing capabilities.

141. The method of claim 134, wherein the gaming machine includes a processing hardware and wherein the operating system in the running step is a version of an operating system that, together with the processing hardware, implements capabilities specified by the Trusted Computing Platform Alliance (TCPA).

142. The method of claim 135, wherein the gaming machine includes a processing hardware and wherein the operating system in the running step is a version an operating system that, together with the processing hardware, implements TCPA, System File Protection and Driver Signing.